151 Southhall Lane, Ste 450
Maitland, FL 32751
P.O. Drawer 200
Winter Park, FL 32790-0200
www.inteserra.com

February 16, 2018
Via ECFS Filing

Ms. Marlene H. Dortch, FCC Secretary
Federal Communications Commission
9050 Junction Drive
Annapolis Junction, MD 20701

RE: Windwave Technologies, Inc.
CY2017 Annual CPNI Certification
EB Docket No. 06-36
Form 499 Filer ID 825276

Dear Ms. Dortch:

Attached for filing is the Calendar Year 2017 CPNI Compliance Certification and Statement of CPNI Procedures and Compliance as required by 47 C.F.R. Section 64.2009 (e) submitted on behalf of Windwave Technologies, Inc.

Any questions you may have regarding this filing should be directed to my attention at 407-740-3031 or via email to Sthomas@inteserra.com. Thank you for your assistance in this matter.

Sincerely,

/s/Sharon Thomas

Sharon Thomas
Consultant

tms: FCCx1801

ST/kf

ANNUAL 47 C.F.R. § 64.2009(e) OFFICER'S CERTIFICATION OF CUSTOMER PROPRIETARY NETWORK INFORMATION (CPNI) COMPLIANCE

EB Docket 06-36

Annual 64.2009(e) CPNI Certification:	Covering calendar year 2017
Name of company(s) covered by this certification:	WindWave Technologies, Inc. d/b/a Windwave Communications
Form 499 Filer ID:	825276
Name of signatory:	Lynn Rodriguez
Title of signatory:	Director of Finance

1. I, Lynn Rodriguez, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. §64.2001 *et seq*.

2. Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in §64.2001 *et seq*. of the Commission's rules.

3. The company has not taken actions (*i.e.*, proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

4. The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

5. The company represents and warrants that the above certification is consistent with 47 C.F.R. §1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

/s/Lynn Rodriguez
Lynn Rodriguez, Director of Finance

February 16, 2018
Date

Attachments: Accompanying Statement explaining CPNI procedures

Statement of CPNI Procedures and Compliance

WindWave Technologies, Inc. ("WindWave") does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. Should WindWave elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

WindWave primarily provides dedicated non-voice services that do not involve call detail information. WindWave offers limited interconnected VoIP services, but does not receive or maintain any call detail associated with the use of the services. Consequently, the CPNI rules related to protection of call detail are not applicable, as WindWave does not have call detail for any of the services it offers. In the event that WindWave provides services in the future that generate associated call detail information, WindWave understands its obligation to protect that information, and will implement appropriate policies and procedures to ensure compliance with the FCC rules.

WindWave understands its obligation to notify law enforcement in the event of a breach of customer's CPNI. If WindWave in the future provides any services that generate call detail information that could be subject to possible disclosure, it will implement appropriate policies and procedures to ensure compliance with the FCC rules with respect to law enforcement and customer notification of such breaches.

Statement of CPNI Procedures and Compliance

Electronet Broadband Communications, Inc. ("Electronet") does not use or permit access to CPNI to market any telecommunications or non-telecommunications services. Electronet has trained its personnel not to use CPNI for marketing purposes. Should Electronet elect to use CPNI in future marketing efforts, it will follow the applicable rules set forth in 47 CFR Subpart U, including, if necessary, the institution of operational procedures to ensure that notification is provided and customer approval is obtained before CPNI is used or disclosed.

Electronet has put into place processes to safeguard its customers' CPNI from improper use or disclosure by employees; and to discover and protect against attempts by third parties to gain unauthorized access to customer CPNI. Electronet maintains all CPNI on a secure server and access by Electronet employees requires a valid username and password.

Electronet does not disclose CPNI to any agents, affiliates, joint venture partners or independent contractors, nor does it use CPNI to identify or track customers who call competing providers. The Company has a strict policy prohibiting the disclosure of CPNI to any third parties, unless required to do so by law (e.g., in response to a subpoena).

Electronet has instituted authentication procedures to safeguard the disclosure of call detail over the telephone, which do not require the use of readily available biographical information or account information as defined by the FCC. Electronet authenticates customers before providing any CPNI over the phone, by requiring them to provide their pre-designated pass phrase, which is not based on readily available biographical information or account information. If the appropriate pass phrase is not provided, Electronet does not disclose call detail over the telephone.

If the customer does not provide the appropriate pass phrase, Electronet will provide CPNI to the customer's address of record, if requested.

A customer who loses or forgets his/her pass phrase can reset the pass phrase by a phone call from the phone number of record with caller self-identifying as one of the listed Authorized Representatives of the account, email from an email account of record and from an Authorized Representative of the account, or letter on customer company letterhead signed by an Authorized Representative, requesting the change. Customer will then be contacted with information about the change.

Electronet does not disclose CPNI on-line. If it elects to do so in the future, it will follow the applicable rules set forth in 47 CFR Subpart U, including the implementation of authentication procedures that do not require the use of readily available biographical information or account information and customer notification of account changes.

Electronet has put into place procedures to notify customers whenever a pass phrase, customer response to a back-up means of authentication for lost or forgotten pass phrases

or address of record is created or changed without revealing the changed information or sending the notification to the new account information. Electronet calls the primary account holder at their phone number of record and follows up with notification that a change as been requested to the customer's email address of record.

Electronet discloses CPNI at its retail location only if the customer has presented a valid photo ID matching his/her account information.

Electronet has adopted procedures to notify law enforcement in the event of a breach of customers' CPNI and to ensure that customers are not notified of the breach before the time period set forth in the FCC's rules, or, if applicable, when so authorized by law enforcement. As soon as practicable, and no later than seven business days upon learning of a breach, the company will notify the U.S. Secret Service and the FBI by electronic means, as required by FCC regulations. Electronet will not notify customers or disclose a breach to the public until seven business days after notification to the U.S. Secret Service and the FBI, unless it believes there is an extraordinarily urgent need to notify customers before seven days to avoid immediate and irreparable harm. In that instance, it will only notify such customers *after* consultation with the relevant investigating agency and will cooperate with the agency's request to minimize any adverse effects of the customer notification. If the Company receives no response from law enforcement after the seventh full business day, it will promptly proceed to inform the customers whose CPNI was disclosed of the breach. The company will delay notification to customers or the public if requested to do so by the U.S. Secret Service or FBI. Notifications to law enforcement and customers are handled by a designated supervisor level employee responsible for managing the company's CPNI compliance.

Electronet maintains written records of any breaches discovered and notifications made to the USSS and the FBI, and to customers.

Electronet has not taken any actions against data brokers in the last year.

Electronet did not receive any customer complaints about the unauthorized release of CPNI or the unauthorized disclosure of CPNI in calendar year 2017.

Electronet has not developed any information with respect to the processes pretexters are using to attempt to access CPNI but does take steps to protect CPNI as described herein.